

EE38061900US

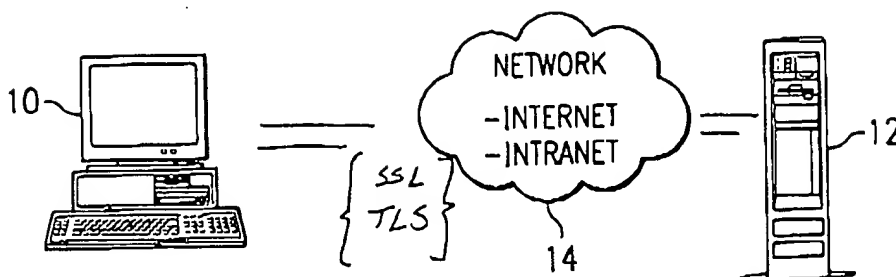


Figure 1

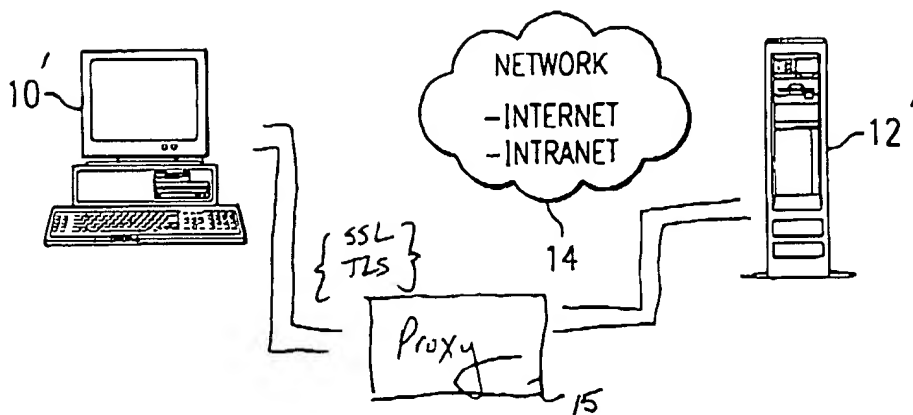


Figure 2

66FEE0"EE928260

Client (1)	Proxy (1)	Client (2)	Proxy (2)	Origin Server
ClientHello				
	ServerHello			
	Certificate*			
	CertificateRequest*			
	ServerKeyExchange*			
Certificate*				
ClientKeyExchange				
CertificateVerify*				
changeCipherSpec				
Finished				
	changeCipherSpec			
	Finished			
		HTTP "connect"		
			Create session ID	
		ClientHello		
				ServerHello
				Certificate*
				CertificateRequest*
				ServerKeyExchange*
		Certificate*		
		ClientKeyExchange		
		CertificateVerify*		
		changeCipherSpec		
		Finished		
Send "master secret" w/ proxy session ID				changeCipherSpec
	Calculate key-block based on "master secret"			Finished
		HTTP Request		
			Update/modify request	
				HTTP content reply
			Transcode reply	
			Send second request	
				HTTP content reply
			(2) ClientHello	
				(2) ServerHello
				(2) Certificate*
				(2) CertificateRequest*
				(2) ServerKeyExchange*
			(2) Certificate*	
			(2) ClientKeyExchange	
			(2) CertificateVerify*	
			(2) changeCipherSpec	
			(2) Finished	
	Notify client of cipher spec change			changeCipherSpec
changeCipherSpec				Finished
Finished			Send third request	
				HTTP content reply
			Transcode final reply	
		Render reply		

Figure 3

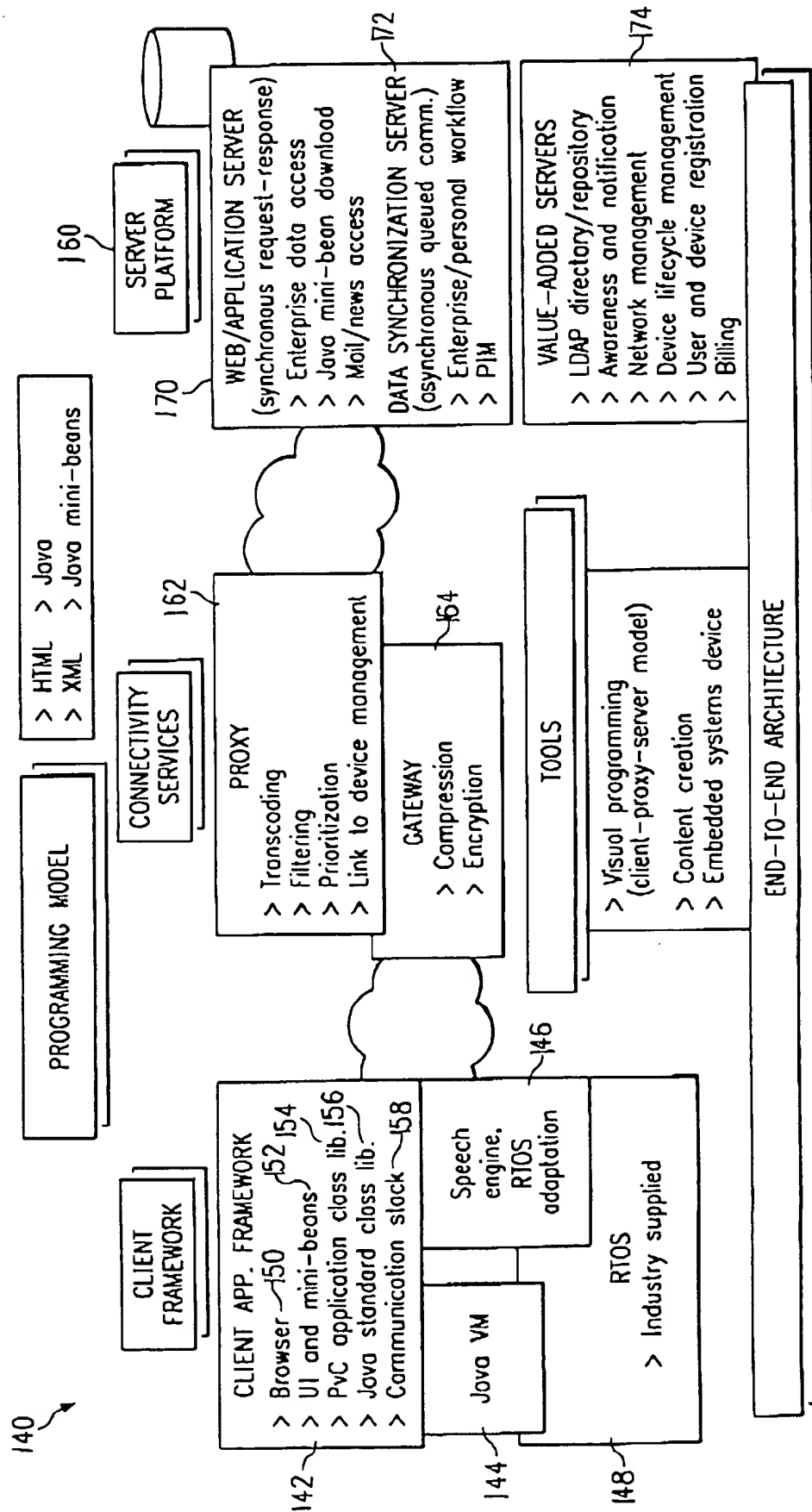


Figure 4